PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-214863
(43)Date of publication of application : 05.08.1994

(51)Int.Cl. G06F 12/00
G06F 9/46
G06F 13/00

(21)Application number : 05-020476
(22)Date of filing : 13.01.1993

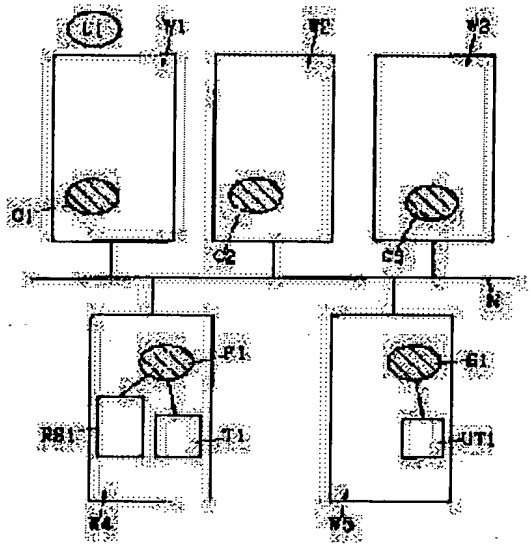
(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : HASHIMOTO SUNAO

(54) INFORMATION RESOURCE MANAGING DEVICE

(57)Abstract:

PURPOSE: To provide an information resource managing device which enables the description of a complicated access limitation concerning the access of information resources, increases the degree of freedom for management, improves security and distributes the management information of information resources and the load of management.

CONSTITUTION: When there is an access request from a client C1 to an information resource RS 1, an information resource managing server F1 checks access right information with an access right information storage table T1 and provides the logic expression of a user group name corresponding to the information resource RS 1 and the classification of access. This logic expression is transmitted to a user group name managing server S1 together with user name information. At the user group name managing server S1, a user group name information storage table UT 1 is retrieved, it is judged whether the user name belongs to the user group or not, the logic expression is checked, and the result is returned to the information resource managing server F1. Thus, the access right is checked.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Dat of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rej ction]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－214863

(43)公開日　平成６年(1994)８月５日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/00	５３７　Ａ	8526－5B		
9/46	３４０　Ｆ	8120－5B		
13/00	３５５	7368－5B		

審査請求　未請求　請求項の数１　ＦＤ　（全　７　頁）

(21)出願番号　特願平5－20476

(22)出願日　平成５年(1993)１月13日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　橋元　直
神奈川県海老名市本郷2274番地　富士ゼロックス株式会社内

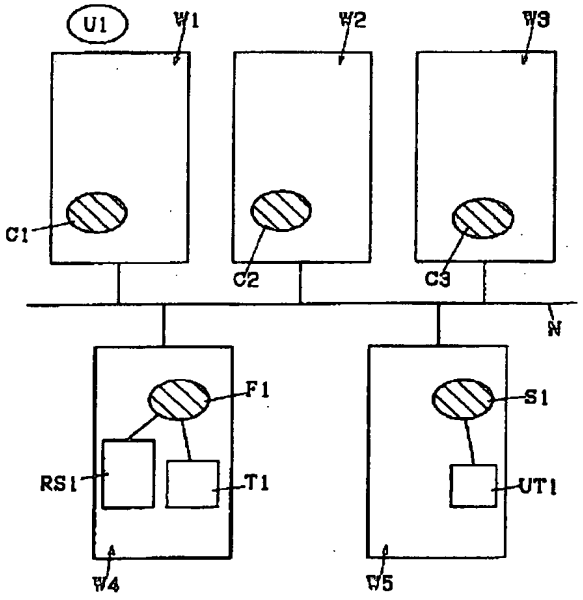
(74)代理人　弁理士　石井　康夫　（外１名）

(54)【発明の名称】　情報資源管理装置

(57)【要約】

【目的】　情報資源のアクセスに関して、複雑なアクセス制限の記述を可能にし、管理の自由度を増加させ、かつ、セキュリティの向上を可能にするとともに、情報資源の管理情報と管理の負荷を分散させた情報資源管理装置を提供する。

【構成】　クライアントＣ１から情報資源ＲＳ１に対するアクセス要求があった場合、情報資源管理サーバＦ１は、アクセス権情報記憶テーブルＴ１によりアクセス権情報をチェックし、情報資源ＲＳ１およびアクセスの種別に対応するユーザグループ名の論理式を得る。この論理式は、ユーザ名情報とともにユーザグループ名管理サーバＳ１に送信される。ユーザグループ名管理サーバＳ１では、ユーザグループ名情報記憶テーブルＵＴ１を検索し、ユーザ名がユーザグループに属するか否かを判定して論理式をチェックし、結果を情報資源管理サーバＦ１に返す。これにより、アクセス権のチェックを行なう。



【特許請求の範囲】

【請求項１】　情報資源のアクセス管理を行なう情報資源管理装置において、情報資源に対するアクセス権、および、ユーザやそのユーザの集合であるユーザグループの名前によって記述される論理式を記憶するアクセス権情報記憶手段と、ユーザグループ名およびユーザグループに含まれるユーザの名前を記憶するユーザグループ名記憶手段を有し、アクセス権情報記憶手段に記憶されているユーザグループの論理式をユーザグループ名記憶手段に記憶されているユーザグループにより評価し、ユーザ名のアクセス権の有無を決定することを特徴とする情報資源管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、共通利用可能な情報資源を管理する情報資源管理装置に関し、特に、情報資源に対するアクセス制御方式に関するものである。

【０００２】

【従来の技術】従来、ローカルエリアネットワークによって複数のワークステーションが相互に接続されたネットワークシステムにおいて、ネットワーク上の情報資源、例えば、ディスク上のファイルや、メモリ上の情報等は、複数の利用者により共用される。このとき、機密保護のため、また、システムの安全性のため、各利用者に対して、または、利用者のグループに対して、それらの情報資源に制限的にアクセスを許可するアクセス権が付与され、アクセス権のない利用者からの当該情報資源に対するアクセスを制限することが行なわれる。

【０００３】従来、このような情報資源のアクセス制限を行なうものとして、アクセス制御リストを用いるものがあった。この方式では、各々の情報資源には、アクセスを許可された利用者あるいは利用者の集合を表すユーザグループのリストが付与されており、情報資源の管理者は、そのリストの中に利用者が入っていればアクセスを許可するものである。この方式は、例えば、前川，所，清水編，「分散オペレーティングシステム」，１９９１，共立出版，ｐｐ１７７－１８２等に記載されている。

【０００４】また、特開平１－２６９５１号公報には、ファイルレベルまたはメンバレベルでアクセスが許可される利用者を設定し、設定されている利用者に対してアクセスを許可する技術が記載されている。特開平２－３５５３５号公報には、ファイル利用者ごとにファイルとのマッピング情報を作成しておき、このマッピング情報を検索することにより、所望のファイルをアクセスする技術が記載されている。この技術では、マッピング情報のないファイルに対しては、アクセスがなされないことから、マッピング情報が一種のアクセス権リストとして機能する。特開平２－２１３２４５号公報には、装置と回線を複数のグループに分類し、各グループごとにグループ情報ビットパターンを設け、さらに各端末及び利用者ごとにアクセス権ビットパターンを設け、グループ情報ビットパターンとアクセス権ビットパターンを比較することにより、アクセスの可否を判定する技術が記載されている。特開平２－２６６４４５号公報には、ユーザ名、パスワードとともにユーザタイプを記憶しておき、ログイン時に入力されたユーザ名からユーザタイプを得て、この情報により、文書データ格納手段へのアクセス権を与える技術が記載されている。さらに、特開平４－４８３５１号公報には、資源情報管理ファイルに利用者を登録しておき、登録されている利用者のみにアクセスを許可する技術が記載されている。

【０００５】このように、資源ごとに利用者を登録したり、利用者ごとに利用できる資源を登録することにより、アクセス制御を行なう技術は、従来より多数開発され、利用されている。

【０００６】しかし、これまでのアクセス制御リストでアクセス制御を行なう方式では、上述のように、リストの各要素は、ユーザ名の集合であるユーザグループと、資源に対する操作との対で表されている。そのため、複数のユーザグループに属す利用者にのみアクセスを許可するといったような複雑なアクセス制御を記述することが困難であった。また、ある情報資源のアクセス制限に関して、あるユーザグループに属する利用者全員から少数の利用者を除いた残りの利用者、すなわち、特定の利用者に対し、アクセスを許可するというような記述ができなかった。さらに、１つのユーザグループに対してアクセス権が与えられているとき、そのセキュリティが破られた場合、そのユーザグループに属していない、アクセス権のない利用者に対してアクセスを許すことになってしまう。

【０００７】また、従来のアクセス制御では、アクセス権の有無のチェックを、その情報資源を管理している情報資源記憶手段だけで行なっている。そのため、管理の負荷が情報資源記憶手段に集中するといった問題や、管理情報が集中しているため故障に対して弱くなるという問題があった。

【０００８】

【発明が解決しようとする課題】本発明は、上述した事情に鑑みてなされたもので、情報資源のアクセスに関して、複雑なアクセス制限の記述を可能にし、管理の自由度を増加させ、かつまたセキュリティの向上を可能にするとともに、情報資源の管理情報と管理の負荷を分散させた情報資源管理装置を提供することを目的とするものである。

【０００９】

【課題を解決するための手段】本発明は、情報資源のアクセス管理を行なう情報資源管理装置において、情報資源に対するアクセス権、および、ユーザやそのユーザの集合であるユーザグループの名前によって記述される論

理式を記憶するアクセス権情報記憶手段と、ユーザグループ名およびユーザグループに含まれるユーザの名前を記憶するユーザグループ名記憶手段を有し、アクセス権情報記憶手段に記憶されているユーザグループの論理式をユーザグループ名記憶手段に記憶されているユーザグループにより評価し、ユーザ名のアクセス権の有無を決定することを特徴とするものである。

【００１０】

【作用】本発明によれば、アクセス権情報記憶手段を、情報資源に対するアクセス権とともに、ユーザグループ名の論理式を記憶するように構成することにより、アクセス制限の複雑な記述を行なうことができる。また、アクセス制限の複雑な記述を行なうことで、情報資源に対するセキュリティを向上させることができる。ユーザグループ名に含まれるユーザ名は、アクセス権情報記憶手段とは別に、ユーザグループ名記憶手段に記憶されているので、アクセス権のチェックをユーザグループ名記憶手段に行なわせることができ、処理の分散化を図ることができる。

【００１１】

【実施例】図１は、本発明の情報資源管理装置の一実施例を含むネットワークシステムの要部の構成を示すブロック図である。図中、Ｎはネットワーク、Ｗ１～Ｗ５はワークステーション、Ｓ１はユーザグループ名管理サーバ、Ｆ１は情報資源管理サーバ、Ｃ１～Ｃ３はクライアント、Ｔ１はアクセス権情報記憶テーブル、ＲＳ１は情報資源、ＵＴ１はユーザグループ名情報記憶テーブル、Ｕ１はユーザである。ワークステーションＷ１～Ｗ５は相互の通信機能を有し、ネットワークＮによって相互に接続され、ネットワークＮのノードとして機能する。

【００１２】ユーザグループ名管理サーバＳ１は、例えば、ワークステーションＷ５で起動される。ユーザグループ名管理サーバＳ１は、ユーザ名、およびその集合であるユーザグループ名が登録されたユーザグループ名情報記憶テーブルＵＴ１を管理する。そして、他のプロセスからのユーザグループ名に関する検索要求に対して、ユーザグループ名情報記憶テーブルＵＴ１を参照して問い合わせに答える。検索の結果、検索要求されたユーザグループ名がユーザグループ名情報記憶テーブルＵＴ１になければ、他のユーザグループ名管理サーバに検索要求を出す。このように、ユーザグループ名管理サーバＳ１は、ネットワークＮ上に複数存在してもよい。

【００１３】情報資源管理サーバＦ１は、例えば、ワークステーションＷ４で起動される。そして、システム内で共通利用可能な情報資源ＲＳ１を保持し、アクセス権情報記憶テーブルＴ１に記憶されているアクセス権情報に基づき、情報資源ＲＳ１を管理する。この情報資源管理サーバＦ１も、ネットワークＮ上に複数存在してもよい。アクセス権情報記憶テーブルＴ１には、情報資源ＲＳ１に対するアクセス権の種類と、ユーザグループ名の論理式との関係情報が保持されている。

【００１４】図１のネットワークシステムでは、情報資源管理サーバＦ１とユーザグループ名情報管理サーバＳ１は別のワークステーションで起動されているが、同じワークステーション内で起動されてもよい。しかし、ワークステーションの負荷を分散させるため、別のワークステーションで起動されることが望ましい。

【００１５】クライアントＣ１，Ｃ２，Ｃ３は、それぞれノードＷ１，Ｗ２，Ｗ３で起動されたプロセスであり、情報資源ＲＳ１のアクセス権を要求するユーザＵ１から起動される。そして、ユーザＵ１とサーバＦ１との間のインターフェースの役割を果たし、例えば、ユーザＵ１からのコマンドの解釈を行ない、情報資源管理サーバＦ１に対して情報資源ＲＳ１へのアクセスの要求を行なう。

【００１６】上述のネットワークシステムの動作を説明する。上述のネットワークシステムでは、ネットワークＮを介して各ワークステーションＷ１～Ｗ５が相互接続され、クライアントサーバ処理方式により、データ処理を分散して行なう。ユーザＵ１は、情報資源ＲＳ１をアクセスするために、例えばワークステーションＷ１上でクライアントＣ１を起動し、クライアントＣ１と情報資源管理サーバＦ１との間で通信を行なわせることによって、情報資源ＲＳ１に対するアクセスを要求する。

【００１７】情報資源管理サーバＦ１は、情報資源ＲＳ１に対するアクセス要求を受けると、アクセス権情報記憶テーブルＴ１を参照することにより、情報資源ＲＳ１と、要求されたアクセスの種類から、アクセスが制限される範囲を示すユーザグループ名の論理式を検索する。そして、情報資源管理サーバＦ１は、ユーザグループ名管理サーバＳ１に対して、検索要求とともにユーザ名Ｕ１と、検索したユーザグループ名の論理式を送信する。

【００１８】ユーザグループ名管理サーバＳ１は、情報資源管理サーバＦ１から、検索要求、ユーザ名、ユーザグループ名の論理式が送られてくると、論理式中の各ユーザグループにユーザが属するかどうかを、ユーザグループ名記憶テーブルＵＴ１を参照して検索する。そして、ユーザ名がユーザグループに属するとき、そのユーザグループを真として論理式を評価し、結果を情報資源管理サーバＦ１に送り返す。

【００１９】情報資源管理サーバＦ１では、ユーザグループ名管理サーバＳ１から返送されてきた結果によって、ユーザＵ１が情報資源ＲＳ１に対してアクセス権があるかどうかを判断し、アクセス要求を処理する。

【００２０】図２は、共通利用可能な情報資源を格納しているワークステーションの要部の詳細図である。図中、図１と同様の部分には同じ符号を付して説明を省略する。ＲＳａ～ＲＳｃは情報資源である。図２に示すように、ネットワークシステムのワークステーションＷ４には、情報資源ＲＳ１の格納ブロックに、例えば、情報

資源ＲＳａ，情報資源ＲＳｂ，情報資源ＲＳｃが格納されている。ここに格納された各々の情報資源ＲＳａ～ＲＳｃは、ネットワークを通して各ワークステーションに対して制限的なアクセスを許可している、共通利用可能な情報資源である。

【００２１】アクセス権情報記憶テーブルＴ１には、これらの情報資源ＲＳａ～ＲＳｃに対応するアクセス権の種類ＡＣ１，ＡＣ２，ＡＣ３と、アクセスが制限される範囲を表すユーザグループ名の論理式ＬＯ１，ＬＯ２，ＬＯ３が、アクセス権情報として格納されている。そして、情報資源管理サーバＦ１は、アクセス権情報記憶テーブルＴ１の各アクセス権情報を参照して、各々の情報資源ＲＳａ～ＲＳｃを管理し、アクセス要求に対する処理を行なう。

【００２２】例えば、情報資源ＲＳａに対して、ユーザＵ１が起動したクライアントＣ１からアクセス権ＡＣ１を必要とするアクセス要求があった場合、情報資源管理サーバＦ１は、情報資源ＲＳａのアクセス権ＡＣ１に対応するユーザグループ名の論理式ＬＯ１を調べ、ユーザＵ１が情報資源ＲＳａに対してアクセス権を有するかどうかを調べる。そのために、検索要求とともに、ユーザグループ名の論理式ＬＯ１とユーザ名Ｕ１をユーザグループ名管理サーバＳ１に対して送信し、アクセス権のチェックを依頼する。

【００２３】図３は、ユーザグループ名管理サーバを有するワークステーションの要部の詳細図である。ユーザグループ名管理サーバＳ１は、ユーザ名、およびその集合であるユーザグループ名を登録したユーザグループ名情報記憶テーブルＵＴ１を管理する。このユーザグループ名情報記憶テーブルＵＴ１は、ユーザグループ名と、そのユーザグループ名に含まれるユーザ名が対応づけられて記憶されている。情報資源管理サーバＦ１から送信されてきたユーザグループ名の論理式ＬＯ１中のユーザグループ名を抽出し、各ユーザグループ名によりユーザグループ名情報記憶テーブルＵＴ１を検索する。検索したユーザグループ名に対応して記憶されているユーザ名の集合に、情報資源管理サーバＦ１から送信されてきたユーザ名Ｕ１が含まれるか否かを判定し、含まれる場合に論理式ＬＯ１中のユーザグループ名を真として、論理式ＬＯ１の論理を判定する。判定結果は、情報資源管理サーバＦ１に送信される。

【００２４】図４は、アクセス情報とユーザグループとの関係の説明図である。図４（Ａ）はアクセス権情報記憶テーブルの一部を示し、図４（Ｂ）は図４（Ａ）に示したアクセス権情報記憶テーブルに記憶されているユーザグループ名の論理式を概念的に示している。

【００２５】アクセス権情報記憶テーブルに、図４（Ａ）に示す情報が記憶されているとき、情報資源ＲＳ１に対するアクセス権ＡＣ１をユーザに与えるためには、ユーザは、ユーザグループ名の論理式「（ＵＧ１＆ＵＧ２）」が表す範囲に属していなければならない。このユーザグループ名の論理式が表す集合を図４（Ｂ）に示している。

【００２６】図４（Ｂ）では、ユーザグループＵＧ１とユーザグループＵＧ２をそれぞれ楕円で示し、ユーザＵ１，ユーザＵ２，ユーザＵ３が集合のどの部分に属するかを示している。ユーザＵ１はユーザグループＵＧ１だけに属し、ユーザＵ３は、ユーザグループＵＧ２だけに属し、ユーザＵ２はユーザグループＵＧ１とＵＧ２の両方に属している。

【００２７】いま、ユーザＵ１が情報資源ＲＳ１に対しアクセスＡＣ１を行なおうとした場合、ユーザＵ１はユーザグループＵＧ１には属するので、ユーザグループ名ＵＧ１は真となるが、ユーザＵ１はユーザグループＵＧ２には属しないので、ユーザグループ名ＵＧ２は偽となり、ユーザグループ名の論理式（ＵＧ１＆ＵＧ２）を満足しない。そのため、ユーザＵ１からのアクセス要求は拒否される。

【００２８】ユーザＵ２が情報資源ＲＳ１に対しアクセスＡＣ１を行なおうとした場合には、ユーザＵ２は、ユーザグループＵＧ１及びユーザグループＵＧ２とも属しているので、ユーザグループ名の論理式（ＵＧ１＆ＵＧ２）を満足する。そのため、ユーザＵ２からのアクセスＡＣ１が実行されることになる。

【００２９】このように、ユーザグループ名の論理式によりアクセス権を付与するため、上述のように２つのユーザグループに含まれる特定の利用者に対してのみ、アクセスを許可するといった複雑なアクセス制御を記述することが可能となる。また、１つのユーザグループ、例えばユーザグループＵＧ１に対してセキュリティが破られたとしても、ユーザグループＵＧ２を満足せず、ユーザグループ名の論理式を満足しないので、アクセスすることはできない。このように、セキュリティを向上させることができる。

【００３０】次に、アクセス権要求処理がネットワーク上でのクライアントＣ１、情報資源管理サーバＦ１、ユーザグループ名管理サーバＳ１の間の通信手順によって、どのように処理されるかを説明する。図５は、情報資源のアクセスを行なうための通信手順の説明図である。

【００３１】ユーザＵ１から、ワークステーションＷ２が保持する情報資源ＲＳ１をアクセスする要求がなされると、クライアントＣ１は、通信手順１において、ワークステーションＷ２上で起動された情報資源管理サーバＦ１に対して、アクセス要求とともに、ユーザ名Ｕ１、アクセス要求の対象となる情報資源の名前ＲＳ１、そのアクセスの種類ＡＣ１を送信する。

【００３２】クライアントＣ１からアクセス要求を受け取った情報資源管理サーバＦ１は、自己が保持するアクセス権情報記憶テーブルＴ１の各アクセス権情報を参照

して検索し、アクセス要求された情報資源ＲＳ１とアクセスの種類ＡＣ１に対応する、ユーザグループ名の論理式ＬＯ１を得る。情報資源管理サーバＦ１は、ユーザグループ名管理サーバＳ１に対して、通信手順２において、検索要求とともに、得られたユーザグループ名の論理式ＬＯ１とユーザ名Ｕ１を送信する。

【００３３】ユーザグループ名管理サーバＳ１は、情報資源管理サーバＦ１から、ユーザグループ名の論理式ＬＯ１とユーザ名Ｕ１が送信されてくると、論理式中の各ユーザグループにユーザが属するかどうかを、自己が保持するユーザグループ名記憶テーブルＵＴ１を参照して検索し、ユーザグループにユーザが属する場合、そのユーザグループを真と考えて論理式を評価し、評価結果を通信手順３において情報資源管理サーバＦ１へ送り返す。

【００３４】情報資源管理サーバＦ１は、ユーザグループ名管理サーバＳ１から返された結果によって、ユーザＵ１が情報資源ＲＳ１に対してアクセス権があるかどうかを判断し、アクセス可能であれば情報資源ＲＳ１をアクセスして、結果を通信手順４でクライアントＣ１に返す。

【００３５】上述のように、情報資源管理サーバＦ１では、ユーザ名がユーザグループ名の論理式を満足するか否かの判定を行なわず、ユーザグループ名管理サーバＳ１により、ユーザグループ名の論理式の判定を行なうので、アクセス権の判定に要する負荷を分散することができる。

【００３６】

【発明の効果】以上の説明から明らかなように、本発明によれば、アクセスを許可する範囲を、ユーザグループ名の論理式で表すことができるため、アクセス制限の範囲の記述が容易になり、かつ、詳細な記述が可能となり、情報資源の管理の自由度が増す。また、複数のユーザグループに所属するユーザにだけアクセスを許可するといった指定ができるので、情報資源のセキュリティを向上させることができる。さらに、アクセス権のチェックをユーザグループ名管理サーバに行なわせることで、アクセス権のチェックに伴う負荷の分散化を図ることができるという効果がある。

【図面の簡単な説明】

【図１】　本発明の情報資源管理装置の一実施例を含むネットワークシステムの要部の構成を示すブロック図である。

【図２】　共通利用可能な情報資源を格納しているワークステーションの要部の詳細図である。

【図３】　ユーザグループ名管理サーバを有するワークステーションの要部の詳細図である。

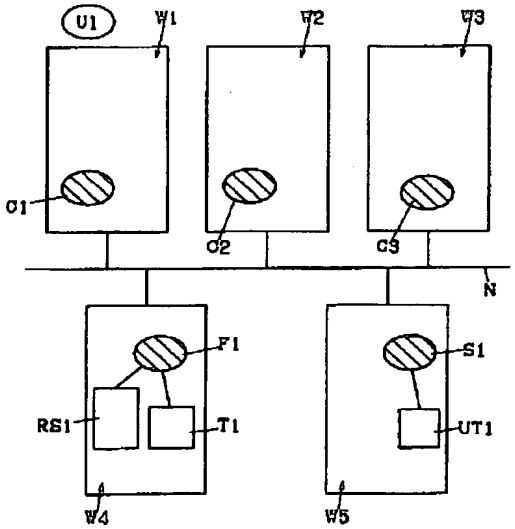
【図４】　アクセス情報とユーザグループとの関係の説明図である。

【図５】　情報資源のアクセスを行なうための通信手順の説明図である。

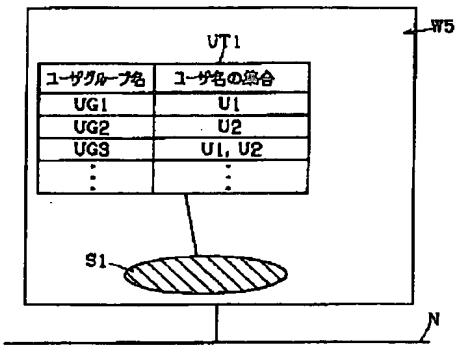
【符号の説明】

Ｎ　ネットワーク、Ｗ１～Ｗ５　ワークステーション、Ｓ１　ユーザグループ名管理サーバ、Ｆ１　情報資源管理サーバ、Ｃ１～Ｃ３　クライアント、Ｔ１アクセス権情報記憶テーブル、ＲＳ１　情報資源、ＵＴ１　ユーザグループ名情報記憶テーブル、Ｕ１　ユーザ。

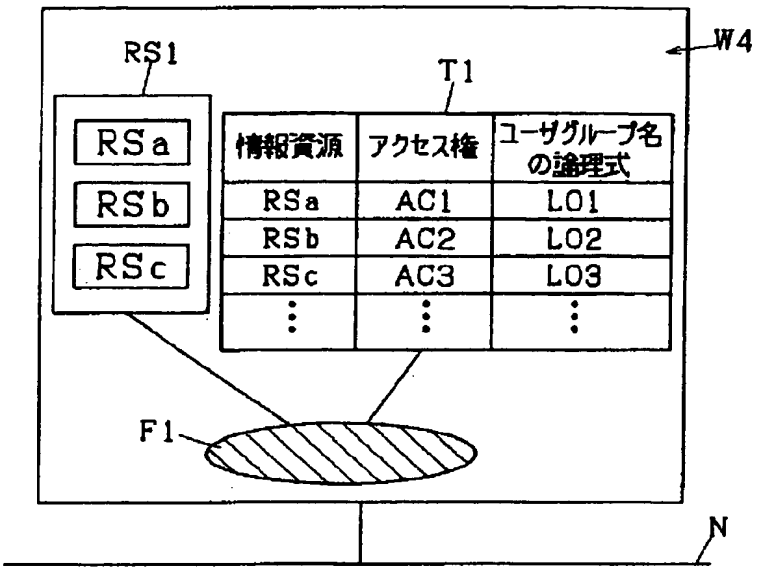
【図１】



【図３】



【図２】

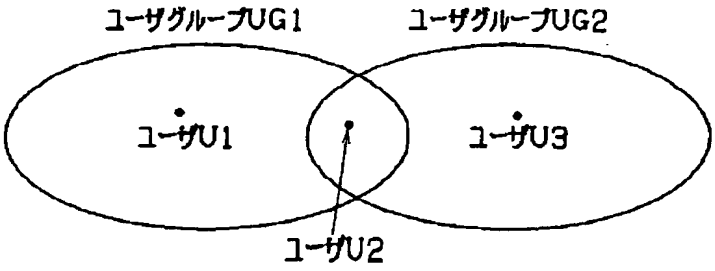


【図４】

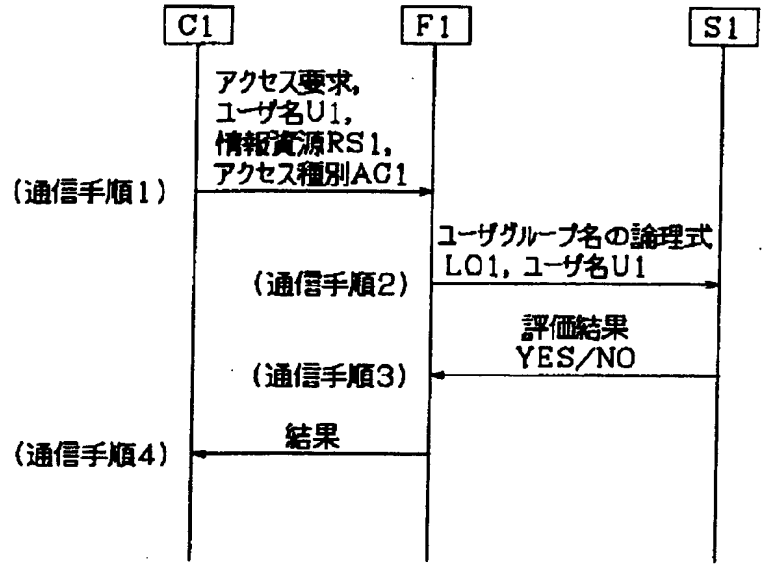
（Ａ）

情報資源	アクセス権	ユーザグループ名の論理式
RS1	AC1	(UG1&UG2)

（Ｂ）



【図５】


C1
F1
S1
アクセス要求,
ユーザ名U1,
情報資源RS1,
アクセス種別AC1
(通信手順1)
ユーザグループ名の論理式
LO1, ユーザ名U1
(通信手順2)
評価結果
YES/NO
(通信手順3)
結果
(通信手順4)